VI. PRISON INDUSTRY AUTHORITY (PIA) COMPUTER USE

I. Supervision of Inmates' Use of Computers

Applicable Policy Sections:
Areas where inmates are authorized to work on computers shall be posted as such. Each computer in a facility shall be labeled to indicate whether or not inmate access is authorized.

No inmate shall have any computer, modem, or terminal in possession within the facility. There shall be no inmate access to a computer outside the inmate's authorized work, vocational, or educational areas.

Inmates shall not access any computer connected to a local area network (LAN), except as approved by the ISO; nor shall inmates access any computer which has any type of direct, outside communication capability, except as provided in Title 15, section 3370(c). No communication capabilities; e.g., telephone lines, data lines, or telephone access punch panels, shall be permitted in any area where inmates are allowed access computers, except as approved by the ISO.

Inmates shall not use or be informed of any computer password. Passwords shall be set only by the supervising staff.

Inmates shall not access or use any computer-based tool or program that is capable of destroying or corrupting stored data.

All facilities with inmates accessing computers in any capacity, including inmate education programs, shall comply with the following procedures:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Areas where inmates are authorized to work on computers shall be posted as such.
- There shall be no communication capabilities such as telephone, computer line, or radio communication devices in the area.
- Inmates shall not have access to utility programs such as Mace, Norton Utilities, or PC Tools.
- Inmates shall not have access to the MS-DOS commands DEBUG, ASSIGN, and ATTRIB.
- A copy of all facility personal computer-based programs, source codes, and documentation shall be forwarded to and maintained by the Institutions Division Automation Support Unit or Parole Automated Systems Unit.
- Inmates performing data entry or word processing in an authorized education or work production area should be supervised by staff persons able to identify and use the computer operating system, software, and application used on the equipment under their supervision.

Institutions Division shall develop and maintain a system to track inmates who have documented, sophisticated computer expertise or histories of computer fraud or abuse. This identified group of inmates shall not be assigned duties involving the use of personal computers.

Inmates shall not have access to any computer containing sensitive or confidential information. In addition, computers containing sensitive or confidential information shall have appropriate hardware or software security measures installed.

Inmates shall not remove diskettes from authorized work areas. An inventory and appropriate controls shall be maintained on all diskettes. Diskettes for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff and appropriate distribution of such output shall be monitored.
(Title 15 Sec 3041.3; DOM Sec 42020.6)

Section A: Physical Verification and Observations ***(To be completed for each Industry)***

1. Are all computers clearly marked with correct signage?

Findings

2. Are inmate work areas clearly marked as such located in such a manner that staff may observe them?

Findings

3. Are there any outside communications devices located in areas where inmates work?

Findings

Section B: Supervisor Interviews

4. Are inmates screened for computer crimes or fraud before hiring?

Findings

5. Are diskettes and other media controlled in accordance with DOM?

Findings

6. Are inmate hard drives and floppy diskettes checked for data integrity and/or misuse on a regular basis?

Findings

7. Do inmates have access to confidential, sensitive or personal information?

Findings

Section C: Network Administrator

8. If inmates use computers connected to a network, are staff using the same network?

Findings

9. What system policies and/or group policies are in place to limit inmate access to only programs they use to complete their assignments?

Findings

10. Are inmates allowed to do administration functions on the server?

Findings

11. Do inmates access shared folders or drives on the network?

Findings

12. How are passwords managed for inmates?

Findings

II. Manufacturing and Planning System (MAPS)

This audit consists of three components:

1. Review of documentation, conducted prior to the on-site activities, it consists of a review of documents provided by the *** and PIA Headquarters operations. Documents provided by the *** are: copies of all MAPS user security agreements, including both staff and inmates, and copies of the MAPS System Administrator and Backup forms. Documents obtained from PIA Headquarters are: Property Unit listing of all MAPS hardware components and PIA Information Systems Division (ISD) listings of all MAPS hardware components, MAPS users, and Access Logs for *** Logon IDs.

2. On-site verification of hardware inventory. All equipment locations and tag numbers will be checked and verified against information maintained at PIA headquarters.

3. Verification of MAPS user logons. All MAPS users will be asked to log on to the MAPS system in the presence of an audit team member. The purpose of this is to confirm that all users are aware of logon procedures and use their own logon IDs.

Following are the findings in each of these areas:

13. MAPS Inventory Findings:

a. ***Do the two MAPS inventory lists, the one from Property Unit, and the one maintained by the ISD that reflects information provided by the *** MAPS System Administrator, correlate with each other? (DOM Sec 46030.1 and Sec 46030.4)***

Findings

b. Are actual locations of MAPS components documented correctly on the ISD listing?
(DOM Sec 46030.1 and Sec 46030.4)

Findings

c. Is the Frame Relay Access Device located in a secure environment?
(Title 15, Section 3041.3)

Findings

14. MAPS User Account and Logon Findings:

a. Are all user IDs current?
(MAPS System Administrator Handbook, Page IV)

Findings

b. Does each user have a current Security form on file?
(MAPS System Administrator Handbook, Page IV)

Findings

c. Were any unauthorized access attempts found during the audit of the Access IDs?
(MAPS Free Staff and Inmate Security Agreement)

Findings

d. Do all users know logon procedures?
(MAPS System Administrator Handbook, Page III)

Findings

e. Are the System Administrator and Backup forms on file and current?
(MAPS System Administrator & Backup Agreement)

Findings

III. Information Security Coordinator

Workgroup Computing - Training
Workgroup management is responsible for ensuring that staff members possess the knowledge and skills necessary for effective use of workgroup computing facilities, and that there is sufficient depth of training to prevent disruption of key activities in the event of unexpected staff changes. At least two staff members should be trained in using each workgroup computing application and the equipment that it uses.

The Workgroup Computing Coordinator shall assist in the identification and scheduling of suitable training and in coordinating the development of training materials to be included as part of new employee orientations.
(DOM Sec 48010.12)

Inventory and Software Licenses
The CDC shall maintain an inventory of its significant microcomputer commodities used for workgroup computing configurations. The inventory shall provide a description of each item (including serial and model numbers of equipment and version numbers of software), its date of acquisition, and the unit to which it is currently assigned. This inventory may be part of CDC's existing inventory system. The CDC shall also maintain inventories of licensed software and significant applications installed on workgroup computing configurations. These inventories will be available for audit purposes.

Software license agreements shall be strictly adhered to. Proprietary software cannot be duplicated, modified, or used on more than one machine, except as expressly provided for in the manufacturer's license agreement Program updates may be downloaded from the Internet in accordance with the owner's license agreement.
(DOM, sec *48010.14 and 48010.10.1)*

Modems
Each facility and parole office is to develop a policy to ensure the security of modems used within that facility or parole office. The policy shall include procedures to ensure that:

- All modems are safeguarded when in use and protected from unauthorized access when not in use. External modem procedures shall include a plan to physically lock external modems when not in use.
- The physical location of each modem is tracked at all times.
- An on-site evaluation of modem use is performed no later than 90 days after installation of each modem installed in a facility. This on-site evaluation shall be conducted by Institutions Division or P&CSD staff, respectively.

It is recommended that modems in facilities be used on dedicated data lines or a basic business line with call detail installed exclusively for modem communications. It is also suggested that an analysis be conducted to assess which type of communications service

is more cost-effective to the user. By assessing the length of time involved in the actual transmission of data and the distance and speed (baud rate) of the transmission, it can be determined which service is most appropriate to use.
(DOM sec 48020.6)

Procurement and Justification

If the procurement request is not covered by the Workgroup Computing Policy, the requesting unit shall complete a Feasibility Study Report (FSR). The Project Initiation Unit located in the Information Systems Branch (ISB) will provide assistance in completing FSRs.

During the acquisition of workgroup computing technologies, a procurement process will follow and/or parallel the workgroup computing authorization process.
Responsibilities of Procurement:

- The necessary procurement documents are completed and the acquisition is completed in conformance with the Public Contract Code and departmental policies and procedures.
- Information technologies procurements have been authorized. For workgroup computing technologies, this means ensuring that the Workgroup Computing Coordinator has an approved CDC Form 1855 on file, and that the procurement documents have appropriately referenced this Form.

(DOM Sections 43020.2, 43020.3.2, 45040.3, 48010.4.8; 48010.8; 48010.8.3)

Employee Information Security Awareness Training and Self-Certification

CDC divisional security coordinators, decentralized end-users, and Local Area Network (LAN) managers are responsible for self-certifying that they are in compliance with applicable CDC information security policies. Responsibility for the dissemination of the policies rests with the owner and the designated security coordinator; responsibility for compliance rests with the end-users.

This policy is intended to ensure compliance by CDC personnel who have been granted access to CDC information resources.

Appropriate decentralized and control entity procedures shall be developed by each CDC division that owns or has custody of decentralized applications. Each such procedure is subject to approval and audit by the ISO. The procedures are constrained by the following:

- A separate statement of self-certification shall be completed for each organizational entity, where applicable.
- Each statement of self-certification shall be signed by a representative of the senior management of the organizational entity.
- Each statement of self-certification is to be filed unless otherwise instructed by CDC's ISO.

(DOM Sec 49020.9.1)

Inmate-Developed Applications

Any computer-based system created by inmate programmers that is used by any entity within the Department to accomplish work shall not be operated by any inmate who created the package.

Institutions Division shall create procedures to safeguard against the situation where an inmate programmer who created a departmental program is allowed to also be the user/operator of the system.
(DOM Sec 49020.19.6)

15. Is there an Information Security Coordinator (ISC) assigned to and working at *** ?
(PIA ISD Policy 200.4)

Findings

16. Does your job description match the description provided for the Information Security Coordinator?
(PIA ISD Policy 200.4)

Findings

17. What training have you received?

Findings

18. How does PIA ensure adherence to software licensing laws?

Findings

19. Are Information Technology acquisitions conducted appropriately?

Findings

20. How are computer use agreements and annual self-certifications for staff maintained?

Findings

21. Are there any inmate-developed programs/databases/screensavers etc. in use? If yes, please describe, including function, who and how they are maintained, and primary user.

Findings

22. ***How are modems maintained at this location?*** *(Note: During the pre-audit document review, the list of modems sent annually to PIA's ISD is reviewed. This list shall be compared to the inventory provided to the OOC prior to the on-site audit, and will be confirmed during the Inventory portion of the on-site audit.)*

Findings

23. Is Internet access allowed from any PIA area? (If yes, please provide copies of approved requests.)

Findings

24. ***Inventory of computer equipment***

The inventory sheets corresponding to all computers are to be provided to the audit team. The team will select from these inventory sheets a number of systems to physically check for correlation between the inventory and the actual system, including physical location, identification numbers, assignee and software installed. A check will be made on each system selected to confirm that no personal software, including games, are installed.

a. Is an inventory maintained?

Findings

b. Is the inventory accurate and current?

Findings

c. Were any unauthorized software, including games, found?

Findings

d. Are CABS directories removed from inmate computers?

Findings

e. Are there communications software or protocols, such as but not limited to, WinFAX, ProCOMM or PC Anywhere, or dial-up networking programs on inmate computers?

Findings

f. Are the proscribed commands (DEBUG, ASSIGN & ATTRIB) removed from all inmate-access computers?

Findings

IV: Information Security Training and Self-Certification.

25. Logon/IDs and Passwords

Access to CDC's dedicated computers is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal, because the password which allowed the session to begin remains in effect throughout the session. Additionally, no ability shall exist for a user to store, load, or invoke the logon process on any CDC computer, by any method that includes the user Resource Access Control Facility (RACF) ID or the password. Violation of this policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those having used the password. User IDs shall never be shared. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what the password is.
- Not write down the password.
- Not use an obvious password.
- Not leave an active terminal session.

(DOM Section 49020.9.2)

A) Do staff have their own logon/ID and personal password?

Findings

B) Are users aware of the necessary measures taken to ensure security and protection of information?

Findings

C) Are users aware of how password changes are handled?

Findings

26. Information Security Awareness Training

All persons who have access to any CDC information shall be provided security awareness training at the time such access begins, and at least annually thereafter.

All individuals having access to CDC information shall be made aware of the background, scope and objectives of CDC's information security program and of specific CDC information security policies and procedures that are applicable to the level and type of access granted to the individual.

All CDC employees shall also be made aware of the events and activities that constitute threats to the organization for which they work, and of the actions to be taken when confronted by those events or activities.
(DOM Section 49020.17)

A) When was the last time the user received security awareness training?

Findings

27. Incident Reporting

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. It is the policy of the Department that the following incidents shall be reported through the chain of command to the departmental ISO:

- Any incidents involving unauthorized access to automated data, automated files, or databases.
- Any incident involving the unauthorized modification, destruction or loss of automated data, automated files, or databases.
- Any incident involving a virus, worm, or other such computer contaminant (see also DOM Section 41010).
- Any incident involving the unauthorized use of computer equipment, automated data, automated files, or databases.
- Any incident involving the misuse of the information assets of the Department.
  (DOM Section 49010.6.2)

A) Are users aware of the type of "actions" which constitute an information security violation or incident which must be reported through the chain of command to the CDC ISO?

Findings

B) Are users aware of the procedure for handing a suspected incident?

Findings

28. Information Integrity

The vast majority of information maintained by CDC is confidential and/or sensitive in nature. Its untimely or unauthorized release external to the organization may have significant, adverse impact on CDC.

Authorized persons engaging in a terminal session with a computer shall log off (terminate the session) before leaving the immediate vicinity of the terminal. User IDs shall never be shared
(DOM Section 48010.9.1, 49020.9.2)

Are there any unattended terminals or workstations with action sessions in the work area visited by the auditor?